#10 WM 2/5/03

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application Serial No. 09/401,251
Filing Date 9/23/1999
Inventor ..... Keene, et al.
Group Art Unit 2172
Examiner ..... Pham, Hung Q.
Attorney's Docket No. AGIL-00500
Confirmation No. 4434
Title: Method and Apparatus for Providing Controlled Access to Software Objects and Associated Documents

APPEAL BRIEF

To: Commissioner of Patents and Trademarks
Washington, D.C. 20231

From: David R. Stevens (Reg. No. 38,626)
Stevens & Sponseller LLP
P.O. Box 1667
San Jose, CA 95109-1667
(408) 288-7588

Pursuant to 37 C.F.R. § 1.192, Applicant hereby submits an appeal brief for application Serial No. 09/401,251, filed September 23, 1999, within the requisite time from the date of filing the Notice of Appeal. Accordingly, Applicant appeals to the Board of Patent Appeals and Interferences seeking review of the Examiner's rejections.

(1) Real Party in Interest

The real party in interest is Agile Software Corporation, the assignee of all right, title and interest in and to the subject invention.

(2) Related Appeals and Interferences

Appellant is not aware of any other appeals or interferences that will directly affect, be directly affected by, or otherwise have a bearing on the Board's decision to this pending appeal.

(3) Status of Claims

Claims 1-16 stand rejected and are pending in this Application. Claims 1-16 in their current form are set forth in the Appendix of Appealed Claims on page 12.

Claims 1-12 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,052,688 to Thorsen (hereinafter "Thorsen").

Claims 13-16 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Thorsen.

(4) Status of Amendments

A Final Office Action was issued on July 17, 2002.

Appellant filed a Notice of Appeal on November 18, 2002, in response to the Final Office Action.

No amendments have been filed subsequent to the Final Office Action of July 17, 2002.

(5) Summary of Invention

The invention provides a database system for storing and providing controlled access to objects and associated documents by multiple users according to predetermined privileges set by the owner, or host, of the stored information. An embodiment of the system 100 is illustrated in Fig. 1 and described in the specification from page 5, line 17 to page 10, line 20. Individual users, or guests, can be given access to the objects, their attributes and associated documents as determined by the host of the information. An example host system 104 is illustrated in Fig. 2 and described in the specification from page 10, line 21 to page 14, line 20. The host of the information can set up access privileges based on any type of relationship. This is particularly useful in complex business relationships between a host and a plurality of users, both of which may be sensitive about their trade secrets and other confidential information. An example information retention system 138 is illustrated in Fig. 4 and described in the specification from page 16, line 20 to page 20, line 18.

In operation, after given an access identification, a user can access the database system and request access to an object. Fig. 8 illustrates an example flow diagram representing operation of the system, which is also described in the specification from page 26, line 1 to page 28, line 9. The system retrieves information pertaining to the individual user's privilege criteria and determines which information contained in the database may be accessed by the requestor. The system then filters the information including objects, their attributes and associated documents according to the privilege information and gives the user limited access to the information. The requested and approved information can then be sent to the requestor of the information. This could

also be displayed to the user as a document file having a redacted document, blocking out the information that the user is not privileged to see.

(6) Issues

1. Whether Claims 1, 6, 7, 10, 11 and 12 are unpatentable over Thorsen when the reference fails to disclose or suggest the limited access of an object that is outside a database.

2. Whether Claims 2, 3, 4, 5 and 8 are unpatentable over Thorsen when the reference fails to disclose or suggest access data application code that allows a user to read the contents of an object according to access privileges associated with the user.

3. Whether Claim 9 is unpatentable over Thorsen when the reference fails to disclose or suggest loading information into a version of an object in separate groups having separate access privilege criteria.

4. Whether Claims 13, 14 and 15 are anticipated by Thorsen when the reference does not disclose transmitting a redacted version of an object that restricts information according to the requestor's user privilege access criteria.

5. Whether Claim 16 is anticipated by Thorsen when the reference does not disclose transmitting a version of an object that was set up according to a user's privilege access criteria in the form of a document file that includes a version of the requested object and a version of associated documents.

(7) Grouping of Claims

All of the claims do not stand or fall together. The claims are grouped as follows:

Group I: Claims 1, 6, 7, 10, 11 and 12.

Group II: Claims 2, 3, 4, 5 and 8.

Group III: Claim 9.

Group IV: Claims 13, 14 and 15.

Group V: Claim 16.

(8) Argument

1. Group I: Claims 1, 6, 7, 10, 11 and 12 are not taught or suggested by Thorsen because Thorsen fails to disclose or suggest the limited access of an object that is outside a database.

According to the invention, direct access to the database is not required. Rather than giving a user limited access to a database, the invention provides a system whereby an application server packages a representation of an object in a document file that contains a version of the object along with representations of any associated documents.

Claim 1 recites, "an application server configured to control access to data stored in the database and to set up and send a document file having a representation of an object and associated documents that are stored in the database". Claim 1 further recites, "access data application code stored in the memory and executable by the application server, the application code being responsive to the access criteria associated with groups of data contained within a version of an object and to predetermined privileges for allowing controlled access to individual groups of data contained within the version of the object by an individual user that was set up to be sent to a user computer system and

that may be viewed by a user according to the user's predetermined privileges on the user computer system." Thorsen discloses a system and method for accessing a database by initiating and maintaining data access nodes and variable access structure. The Thorsen disclosure describes a system that provides direct access to the database and that maintains access structures within the database. Thorsen does not disclose or suggest accessing database data via an object that is outside the database. The Thorsen disclosure focuses on direct access to the database and fails to suggest the type of data access through an object as recited in Claim 1. Thus, Thorsen fails to disclose or suggest the limited access of an object that is outside a database.

2. Group II: Claims 2, 3, 4, 5 and 8 are not taught or suggested by Thorsen because Thorsen fails to disclose or suggest access data application code that allows a user to read the contents of an object according to access privileges associated with the user.

Claim 2 depends from Claim 1 and, therefore, includes the limitations of Claim 1. Claim 2 recites, "the access data application code enables the ability of a user to read the contents of the transferred version of the requested object that was sent by the application server according to access privileges associated with the user." Thus, Claim 2 further describes that the object sent to the user is based on access privileges associated with the user.

As discussed above, Thorsen does not disclose or suggest accessing data via an object that is outside the database. Further, Thorsen does not disclose providing an object based on access privileges associated with the user. Since Thorsen fails to disclose the use of an object as recited in Claim 2, Thorsen makes no reference or suggestion to an

object that is based on a user's access privileges. Thus, Thorsen fails to disclose or suggest access data application code that allows a user to read the contents of an object according to access privileges associated with the user.

3. Group III: Claim 9 is not taught or suggested by Thorsen because Thorsen fails to disclose or suggest loading information into a version of an object in separate groups having separate access privilege criteria.

Claim 9 depends from Claim 7 and, therefore, includes the limitations of Claim 7. Claim 9 recites, "establishing a version of an object includes loading information into the version of the object into separate groups having separate access privilege criteria." Thus, Claim 9 describes that a particular object may include different groups of information with different access criteria. Thus, different users with different access privileges may obtain different information from the same object.

As discussed above, Thorsen does not disclose or suggest accessing data via an object that is outside the database. Further, Thorsen does not disclose the use of an object containing different groups of information having different access criteria. Since Thorsen fails to disclose the use of this type of object, there is no suggestion in Thorsen to include an object with groups of information having different access criteria. Thorsen describes a system that provides direct access to a database rather than a system using objects containing groups of information with different access criteria, as claimed in Claim 9. Thus, Thorsen fails to disclose or suggest loading information into a version of an object in separate groups having separate access privilege criteria.

4. Group IV: Claims 13, 14 and 15 are not anticipated by Thorsen because Thorsen fails to disclose transmitting a redacted version of an object that restricts information according to the requestor's user privilege access criteria.

Claim 13, for example, recites, "computer readable code means for transmitting a version of the requested object in the form of a redacted document that masks information according to the requestor's user privilege access criteria." As discussed above, Thorsen does not disclose accessing data using an object that is outside the database. Further, Thorsen does not disclose transmitting a redacted version of an object that restricts information. Although Thorsen discloses a system that provides direct access to a database, the reference fails to disclose all elements of Claims 13, 14 and 15. Accordingly, Claims 13, 14 and 15 are not anticipated by Thorsen because Thorsen fails to disclose transmitting a redacted version of an object that restricts information according to the requestor's user privilege access criteria.

5. Group V: Claim 16 is not anticipated by Thorsen because Thorsen fails to disclose transmitting a version of an object that was set up according to a user's privilege access criteria in the form of a document file that includes a version of the requested object and a version of associated documents.

Claim 16 recites, "setting up a version of an object and associated documents according to user access privileges for transmission to the user; and transmitting a version of the requested object that was set up according to the requestor's user privilege access criteria in the form of a document file that includes a version of the requested object and a version of associated documents via the network." As discussed above, Thorsen discloses a system that provides direct access to a database. In contrast, the language of Claim 16

includes transmitting an object to a user where the object is set up based on the user's access privileges. Thorsen does not disclose the use of an object that is set up based on a user's access privileges. Thus, Thorsen fails to disclose all elements of Claim 16. Accordingly, Claim 16 is not anticipated by Thorsen because Thorsen fails to disclose transmitting a version of an object that was set up according to a user's privilege access criteria in the form of a document file that includes a version of the requested object and a version of associated documents.

Conclusion

The Office's basis and supporting rationale for the § 103(a) and § 102(e) rejections is not supported by the teaching of the cited references. As discussed above, regarding the claims in Group I, Thorsen does not disclose or suggest the limited access of an object that is outside a database. Regarding the claims of Group II, Thorsen fails to disclose or suggest access data application code that allows a user to read the contents of an object according to access privileges associated with the user. With respect to the Group III claim, Thorsen fails to disclose or suggest loading information into a version of an object in separate groups having separate access privilege criteria. In the Group IV claims, Thorsen fails to disclose transmitting a redacted version of an object that restricts information according to the requestor's user privilege access criteria. Regarding the claim of Group V, Thorsen does not disclose transmitting a version of an object that was set up according to a user's privilege access criteria in the form of a document file that includes a version of the requested object and a version of associated documents.

Applicant respectfully requests that the rejections be overturned and that pending Claims 1-16 be allowed to issue.

Respectfully Submitted,

Dated: _____ By: _____
David R. Stevens
Reg. No. 38,626

(9) Appendix of Appealed Claims

1. A system for providing the transfer of and the controlled access to a version of an object and other associated information a file by a plurality of users comprising:

a database for storing an object and associated information, the object comprising distinguishable groups of data, each group of data having associated access criteria for access to the groups of data;

an application server configured to control access to data stored in the database and to set up and send a document file having a representation of an object and associated documents that are stored in the database ;

a memory for storing software code for controlling the operation of the application server;

access data application code stored in the memory and executable by the application server, the application code being responsive to the access criteria associated with the groups of data contained within a version of an object and to predetermined privileges for allowing controlled access to individual groups of data contained within the version of the object by an individual user that was set up to be sent to a user computer system and that may be viewed by a user according to the user's predetermined privileges on the user computer system.

2. A system according to Claim 1, wherein the access data application code enables the ability of a user to read the contents of the transferred version of the requested

object that was sent by the application server according to access privileges associated with the user.

3. A system according to Claim 2, wherein the access data application code includes the ability to modify the contents of the version of the requested object.

4. A system according to Claim 3, wherein the ability to modify includes the ability to delete information contained in the version of the requested object.

5. A system according to Claim 3, wherein the ability to modify includes the ability to add data to the version of the requested object.

6. A system according to Claim 1 wherein the access to the version of the object is determined by a business relationship to produce products and defined by the host according to the need of information in the product chain, and wherein the transferred version of the object is configured to reveal limited information according to a guest user's predetermined access privileges.

7. A method of controlling access to objects stored in electronic form, comprising:

storing an object, the object comprising distinguishable groups of data, each group of data having associated access criteria for access to the groups of data;

controlling the access to the database using an application server, that is configured to set up a version of an object according to access criteria established for a user;

storing software code for controlling the operation of the CPU in memory;

transferring a version of an object to a user in the form of a document file having the version of the object and any associated documents requested by a user contained therein; and

allowing controlled access to individual groups of data contained within the transferred version of the object by an individual user according to an individual user's predetermined privileges in response to the access criteria associated with the groups of data contained within the version of the object transferred to the user and to a user's predetermined privileges.

8. A method according to Claim 7 further comprising:

receiving an object request by a requestor;

verifying the requestor's user privilege access criteria; and

transmitting a version of an object configured to reveal information contained with in the version of the object according to the requestor's user privilege access criteria.

9. A method according to Claim 7, wherein establishing a version of an object includes loading information into the version of the object into separate groups having separate access privilege criteria.

10. A method according to Claim 7, wherein establishing privilege access criteria includes identifying the separate groups of information to which the user may access for use in setting up a version of the object to be sent to the user in response to the user request .

11. A method according to Claim 7, wherein verifying the requestor's user privilege access criteria includes extracting the requestor's user identification from the object request, verifying the requestor's user identification and identifying the groups of data within the version of the object to which the requestor has access.

12. A method according to Claim 7, further comprising transmitting a redacted version of an object by sending an electronic object to the requestor that contains the groups of information to which the requestor has access to and that excludes groups of information associated with an object to which the requestor does not have access.

13. A computer program product for use with a computer system, a central processing unit and means coupled to the central processing unit for storing a database to automatically manage objects for viewing and marking an object having varying formats without the use of any originating application of a file to view the object, comprising:

computer readable code means for establishing an object in a storage location;

computer readable code means for identifying a user to have limited access to information associated with the object;

computer readable code means for establishing privilege access criteria that define the scope of access of a version of the object for the user;

computer readable code means for receiving an object request by a requestor;

computer readable code means for verifying the requestor's user privilege access criteria; and

computer readable code means for transmitting a version of the requested object in the form of a redacted document that masks information according to the requestor's user privilege access criteria.

14. A computer program device, comprising:

a computer program storage device readable by a digital processing apparatus;

a program stored on the program storage device and including instructions executable by the digital processing apparatus for controlling the apparatus to perform a method of managing documents for viewing and modifying an object to allow a user to view and modify a version of the object stored in the file, comprising:

establishing an object in a storage location;

identifying a user to have access to the object;

establishing privilege access criteria that define the scope of access of a version of the object for the user;

receiving a object request by a requestor;

verifying the requestor's user privilege access criteria; and

transmitting a redacted version of a requested object in the form of a document file containing the version of the requested object that was filtered according to the requestor's user privilege access criteria.

15. In a computer server having a data base for storing data pertaining to product information, a method of securely transferring data between a source and an access destination comprising:

establishing an object in a storage location;

identifying a user to have limited access to the object;

establishing privilege access criteria that define the scope of access of a version of the object for the user;

receiving a object request by a requestor;

verifying the requestor's user privilege access criteria;

setting up a version of an object and associated documents according to user access privileges for transmission to the user; and

transmitting a redacted version of the requested object that set up according to the requestor's user privilege access criteria, wherein the access criteria defines the information in which a user has privileges of access to the version of the requested object.

16. In an application server having access to a data base for storing objects and associated documents, a method of securely transferring a version of an object and associated documents from the application server to a user system via a network comprising:

establishing privilege access criteria that define the scope of access permitted to a user of a version of an object that may be set up and sent to the privileged user;

receiving a object request by a user via a network for access to a version of an object to which the user has access privileges;

verifying the requestor's user privilege access criteria;

setting up a version of an object and associated documents according to user access privileges for transmission to the user; and

transmitting a version of the requested object that was set up according to the requestor's user privilege access criteria in the form of a document file that includes a version of the requested object and a version of associated documents via the network.